Mission: Compliance and Maturity

COMPLIANCE FRAMEWORKS

BloodHound Federal enables compliance for frameworks that require users to maintain separate privileged accounts from their standard user accounts. Example compliance frameworks include:

NIST CSF v1.1

PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes

- PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties

NIST CSF 2.0

- PR.AA-05: Access permissions, entitlements, and authorizations are defined in a policy, managed, enforced, and reviewed, and incorporate the principles of least privilege and separation of duties
- ID.RA-03: Internal and external threats to the organization are identified and recorded

NIST SP 800-53 Rev. 5

- AC-5: Separation of Duties
- AC-6: Least Privilege

MATURITY MODELS

BloodHound Federal provides Optimal Visibility, Analytics, and Risk Assessment maturity to your organization for implementing Zero Trust for Identities.

CISA *Zero Trust Maturity Model, Version 2.0, April 2023*

- Section 5.1 Identity, Function - Risk Assessment, Maturity Level Optimal, "Agency determines identity risk in real time based on continuous analysis and dynamic rules to deliver ongoing protection."
- Section 5.1 Identity, Function - Visibility and Analytics Capability, Maturity Level Optimal, "Agency maintains comprehensive visibility and situational awareness across enterprise by performing automated analysis over user activity log types, including behavior-based analytics."

DoD *Zero Trust Strategy, October 2022*

- Target Level - User: 1.1 User Inventory (Satisfies)
- Target Level - User: 1.2 Conditional User Access (Enables/Validates)
- Target Level - User 1.4 Privileged Access Management (Enables/Validates)
- Target Level - User: 1.7 Least Privileged Access (Satisfies)